Documentation: Running Nmap Command Executor Web App

This guide will walk you through setting up and running the **Nmap Command Executor** web application. The app allows users to run different Nmap scans via a web interface and optionally save the scan results.

Prerequisites:

#1. Apache Web Server:
You will need Apache installed on your system to serve the web application.

```
sudo systemctl start apache2  # For Ubuntu/Debian
sudo systemctl start httpd    # For CentOS/RHEL
```

#2. PHP:
The application uses PHP to process Nmap scans, so PHP must be installed. You can install PHP along with Apache if not already done.

Install PHP

```
sudo apt install php libapache2-mod-php
```

Verify PHP installation:

```
php -v
```

#3. Nmap:
Nmap should be installed on the server where this app is hosted. To install Nmap:

```
sudo apt install nmap #ubuntu/debian
sudo yum install nmap   #centos/red hat
```

Setting Up the Application:

Create the Folder Structure: You must set up a folder to host the application inside your Apache server's root directory. By default, Apache's web root is `/var/www/html`.

- **Navigate to the Apache root directory**: `cd /var/www/html`
- **Create a folder called `nmapcode`**: `sudo mkdir nmapcode`
- **Set proper ownership for the Apache user (usually `www-data` or `apache`)**:

```
sudo chown -R www-data:www-data /var/www/html/nmapcode # For
Ubuntu/Debian
sudo chown -R apache:apache /var/www/html/nmapcode # For CentOS/RHEL
```

Create the Required Folders:
Inside the `nmapcode` folder, create the following structure:

- **index.php**: This is where the main code goes.
- **scans/**: This folder will store the scan result files. Command to create the `scans` directory:

```
sudo mkdir /var/www/html/nmapcode/scans
```

Upload the PHP Code:
Place the provided PHP and HTML code inside a file called `index.php` in the `nmapcode` folder:

- Command to create the file: `sudo nano /var/www/html/nmapcode/index.php`
- Paste the entire PHP code you provided into this file and save it.

Set Folder Permissions:
The `scans` folder needs to be writable by the Apache web server to store scan results. Set appropriate permissions using:

```
sudo chmod 775 /var/www/html/nmapcode/scans
sudo chown -R /var/www/html/nmapcode/scans  # Ubuntu/Debian
sudo chown -R /var/www/html/nmapcode/scans      # CentOS/RHEL
```

Configuring Sudo Permissions for Nmap:

By default, Nmap requires `sudo` privileges to run certain scans. You can allow Apache to run Nmap with elevated privileges by modifying the `sudoers` file to avoid entering a password every time.

1. **Edit the Sudoers File**: Open the sudoers file to grant Apache permission to run Nmap commands without a password:

```
sudo visudo
```

2. **Add the Following Line**:
   Depending on your system, add one of the following lines to the sudoers file:

```
www-data ALL=(ALL) NOPASSWD: /usr/bin/nmap   #For Ubuntu/Debian
apache ALL=(ALL) NOPASSWD: /usr/bin/nmap       #For CentOS/RHEL
```

This will allow the web server to run Nmap without being prompted for a password.

Accessing the Application:

Start/Restart Apache:
After setting up the files, ensure Apache is running or restart it:

```
sudo systemctl restart apache2   #Ubuntu/Debian
sudo systemctl restart httpd #CentOS/RHEL
```

Access the Application via Web Browser:
Open your browser and navigate to:

http://<server-ip>/nmapcode/

Replace `<server-ip>` with the IP address of your server (or `localhost` if running on a local server).

Using the Application:

- **Target IP/Domain**: Enter a valid IP address or domain name to scan.
- **Nmap Command**: Select the desired Nmap scan from the dropdown menu.
- **Save Results**: Check this option if you want to save the scan results. Saved results will be stored in the `/nmapcode/scans` directory.
- **Run Scan**: Press the "Run Nmap Scan" button to execute the scan.

Logs and Scan Files:

- **Scan Results**: If the user opts to save scan results, the output will be saved as a `.txt` file in the `/var/www/html/nmapcode/scans` directory. The file can be downloaded directly from the interface.
- **Error Logs**: Any issues encountered will be displayed in the web interface, and Apache logs can be checked for further troubleshooting.

Security Considerations:

- **Restricted Access**: Ensure this application is used in a secure environment since it allows Nmap scans. Limit access to trusted users.
- **Input Validation**: While some input validation is provided, be cautious of malicious inputs and always test in a secure environment before deploying publicly.

Troubleshooting:

1. **Permission Denied Errors**: If you encounter permission errors, ensure the `nmap` command is allowed to be run by the web server using `sudo` without a password.
2. **No Scan Output**: Check Apache's error log at `/var/log/apache2/error.log` (or `/var/log/httpd/error_log` on CentOS/RHEL) to identify issues.

This concludes the setup for the **Nmap Command Executor**. You should now be able to run Nmap scans from your web browser and save the results!

If you encounter any problems during setup or use, feel free to reach out to us through our Telegram community for assistance. We're here to help! : t.me/codelivly_chat